

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

----- x
UNITED STATES OF AMERICA,

- against -

10 Cr. 1082 (TPG)

MOHAMMAD SHABAZ KHAWAR,

Defendant.

----- x

SENTENCING MEMORANDUM OF THE UNITED STATES OF AMERICA

PREET BHARARA
United States Attorney for the
Southern District of New York
One Saint Andrew's Plaza
New York, New York 10007
Telephone: (212) 637-1945/2482
Facsimile: (212) 637-2452
E-mail: matthew.schwartz@usdoj.gov
negar.tekeei@usdoj.gov

MATTHEW L. SCHWARTZ
NEGAR TEKEEI
Assistant United States Attorneys
- Of Counsel -

The United States of America (the “Government”), by and through its attorney Preet Bharara, United States Attorney for the Southern District of New York, respectfully submits this memorandum in advance of the sentencing of Mohammad Shabaz Khawar (“Khawar” or the “defendant”) in the above-captioned case, presently scheduled for April 29, 2014, at 4:30 p.m.

PRELIMINARY STATEMENT

Mohammad Shabaz Khawar was part of an international conspiracy that was responsible for stealing financial information from hundreds of thousands of consumers, and then using that stolen information to withdraw tens of millions of dollars from its victim’s accounts. Khawar personally recruited others into the conspiracy, and on at least two occasions, lead teams of co-conspirators that travelled from the United Kingdom to the Netherlands in order to steal consumers’ bank account data from retail locations throughout Holland. And when Khawar was arrested in the Netherlands in 2011, he lied to both Dutch and United States authorities about his role in the fraud. In view of the significant role that Khawar played in this massive fraud, the Government respectfully submits that Khawar should be sentenced within the stipulated Guidelines range of 70 to 87 months’ imprisonment.

BACKGROUND

A. The Scheme to Defraud¹

From at least 2007 until at least the summer of 2011, the Khan Family Organization was an international criminal organization principally in the business of stealing credit card, bank account, and related financial information from consumers at retail establishments; using the

¹ The facts in this section are drawn from Khawar’s Presentence Investigation Report (“PSR”), as well as from the second superseding Indictment in this case, *United States v. Irfan Khan, et al.*, No. S2 10 Cr. 1082 (TPG).

stolen account information to extract cash from automated teller machines (“ATMs”) using counterfeit ATM cards; and laundering the proceeds of the scheme back to its organizers. (PSR ¶ 19; Ind. ¶¶ 2, 84). The Khan Family Organization (or simply, the Organization) — which has at various times been based out of the United Kingdom, the United Arab Emirates, and the Netherlands — developed an especially technologically sophisticated method of fraudulently obtaining customer account data from retail locations. (Ind. ¶ 3). As described below, members and associates of the Organization were dispatched throughout the United Kingdom, mainland Europe, and elsewhere to install credit card reader devices that had been customized to steal users’ account information, through the addition of particularly advanced “skimmers.” (PSR ¶¶ 19; Ind. ¶ 3).

The Organization’s leadership then dispatched members and associates throughout the world — including to New York City, the United Kingdom, mainland Europe, Southeast Asia, the Middle East, Africa, the Caribbean, South America, Australia, and elsewhere — to create counterfeit ATM cards using the stolen account information and to fraudulently withdraw cash from victims’ accounts. (Ind. ¶ 4). Members and associates of the Organization then laundered the proceeds of the fraud back to its leadership through various means, including by physically carrying cash internationally; through structured Western Union or similar transactions; and through the informal system of banking known as hawala or its functional equivalent. (Ind. ¶ 5).

To the Government’s knowledge, the Khan Family Organization was one of the largest, if not the single largest, credit card skimming syndicates throughout the world. Using extraordinarily sophisticated technology, the Organization began to mass produce its skimmers for installation into bank-card readers (also known as PIN Entry Devices, or “PEDs”) in retail

locations throughout Europe. (Ind. ¶ 33). The evidence gathered during the course of the Government's investigation reveals the Organization's enormity:

- In 2008, a member of the Organization's leadership contacted various electronics and software purveyors in Britain to source component parts to manufacture the Organization's skimmers, ordering, for example, 900 modems and 1,300 circuit boards. (Ind. ¶¶ 34-36).
- Between April 2008 and March 2009, a secure FTP site used by the Organization to receive the text messages containing stolen accounts and PINs received approximately 350,000 transfers of data, representing approximately the number of accounts compromised by the Organization over that period. (Ind. ¶ 48).
- In early 2009, a pair of police seizures from Organization premises in London resulted in the seizure of almost a thousand PEDs in various stages of alteration. (Ind. ¶¶ 37-41).
- In early 2010, two co-conspirators were arrested in Holland carrying a memory device that contained, among other things, approximately 186,000 unique stolen bank account numbers and their associated PINS. (Ind. ¶ 67).

In short, the Organization operated on a massive scale.

B. The Defendant's Offense Conduct

As described in the Indictment, after the Organization's original leadership was imprisoned in early 2010, Khawar worked with its new leadership to perpetuate the fraud. On at least two occasions in the Spring of 2011, Khawar recruited teams of co-conspirators and led them on trips from the United Kingdom to Holland, for the purpose of installing manipulated bank-card readers designed to steal consumer's financial information.

In March 2010, Khawar recruited a friend (referred to in the Indictment as CC-5), and the pair travelled to the Netherlands, where they met two other co-conspirators (CC-6 and CC-7). While in Holland, they stole the card-reader device from at least one retail location in Amsterdam – a Vodafone shop – and another at a retail location in Rotterdam. After Khawar

stole the Rotterdam PED, he brought it to another co-conspirator, who altered it so that it would capture customers' bank data, and then surreptitiously replaced it in the store the following day.² (Ind. ¶¶ 79-80). At some point, however, the Dutch authorities became alerted to Khawar's conduct, and attempted to arrest him and his co-conspirators. Ultimately, CC-5 was arrested by the Rotterdam Police, but Khawar was able to escape back to England.

The very next month, however, Khawar recruited a new team and returned to the Netherlands. In April 2011, Khawar traveled from the United Kingdom to the Netherlands, along with his co-defendants Fassel Azim and Abdul Qayam Durrani (both of whom previously pleaded guilty), and David Ashley Smith (who remains a fugitive). (PSR ¶ 30; Ind. ¶ 81). They brought with them, among other things, a laptop computer that contained financial information about more than 15,000 bank accounts stolen a year earlier by other co-conspirators in Holland, and skimmers built to the Organization's specifications. (PSR ¶¶ 28, 31; Ind. ¶ 81). Once in the Netherlands, Khawar, Azim, Durrani, and Smith also obtained three PED terminals, to use as non-functioning dummies. *Id.* In the Netherlands, Khawar, Azim, Durrani, and Smith entered several stores to install manipulated card readers, including a shoe store in Utrecht. *Id.*

In addition, the Organization's new leadership continued to trust Khawar in his supervisory role. For example, in addition to recruiting the other members of the teams that he commanded (and paying their expenses), Khawar was in constant contact with the Organization's leadership in England and its engineers in the Netherlands. Khawar was also trusted to acquire and mail matching SIM cards to the United Kingdom, so that the

² By installing a skimmer in even a single card-reader, the Organization could steal the financial data of thousands, or even tens of thousands, of consumers.

Organization's leadership could receive the stolen bank data once it started to transmit. In addition, it was Khawar who obtained a "top up" card to add credit to the pre-paid phone that the Organization's original leader was using in his Dutch prison. (Ind. ¶ 83).

Ultimately, however, Khawar, Durrani, and Smith were arrested by Dutch authorities after they were found to be in possession of several PEDs, skimmers, and a laptop computer containing information about tens of thousands of stolen bank accounts, including account numbers and PINs. (Ind. ¶ 81).

C. Khawar's Post-Arrest Statements

After his arrest, Khawar spoke at length to both Dutch and American authorities. (PSR ¶ 35-36). Specifically, in June 2011, Khawar was interviewed in the Netherlands by United States law enforcement. Khawar was read and waived his *Miranda* rights at the start of this interview, and he was also represented by counsel throughout the interview.

During the course of that interview, Khawar admitted his own guilt, but falsely denied his leadership role in the Organization. Specifically, whereas Khawar in fact had recruited others to travel with him to the Netherlands in order to further the Organization's aims, he falsely claimed that he had been recruited by one of his co-conspirators.³ Khawar falsely claimed that one of his co-conspirators had brought the physical evidence seized upon his arrest – the skimmers; the laptop containing tens of thousands of stolen accounts; and the top-up card for the jail cell phone – when in fact he was the one who brought it. In general, Khawar both falsely minimized his own involvement in the conspiracy, and provided false information to the

³ In his sentencing submission, Khawar asserts that "[a]fter he left college, he was recruited into the conspiracy by friends he knew from his neighborhood." (Def. Mem. at 3). This is presumably not a reference to the original person that Khawar falsely claimed had recruited him (but who he, in fact, later recruited himself), but to others. If that is so, there is no evidence to support it.

Government about the conduct of others.

The Government can provide further detail about Khawar's statements should the Court desire.

D. The Indictment, Khawar's Extradition to the United States, and His Guilty Plea

On or about September 1, 2011, a grand jury in this District returned the S1 Indictment, charging Khawar in four counts, including conspiracy to commit bank and wire fraud, conspiracy to commit access device fraud, conspiracy to commit international money laundering, and aggravated identity theft. (S1 10 Cr. 1082 (S1 Indictment) ¶¶ 1, 7, 15, 18). On or about July 13, 2012, Khawar was extradited from the United Kingdom to the United States to face these charges.⁴ On or about November 15, 2013, a grand jury in this District returned the S2 Indictment, charging Khawar in the same four counts. (PSR ¶¶ 1-13). On February 26, 2014, Khawar pleaded guilty before Your Honor, pursuant to a plea agreement. (PSR ¶ 14).

E. The Undisputed Guidelines Calculation

Under the terms of the plea agreement, Khawar was permitted to plead guilty to Count Four, which charges conspiracy to commit access device fraud. The parties also agreed on the application of the United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.").

As set forth in the plea agreement, the Guidelines calculation is as follows:

⁴ In his sentencing submission, Khawar asks the Court to consider his Dutch imprisonment when it sentences him. Under 18 U.S.C. § 3585(b), in calculating a sentence, "[a] defendant shall be given credit toward the service of a term of imprisonment for any time he has spent in official detention prior to the date the sentence commences . . . as a result of the offense for which the sentence was imposed . . . that has not been credited against another sentence." This calculation is done by the Bureau of Prisons, however, and should not be incorporated into the defendant's sentence by, for example, reducing his sentence by the time spent imprisoned abroad. *See, e.g., United States v. El-Jassem*, 819 F. Supp. 166, 182 (E.D.N.Y. 1982) (Weinstein, J.) ("Defendant will receive credit for time served in Italy [awaiting extradition] in accordance with United States federal lenient practice. The computation of time served will be made by the Attorney General." (citing *United States v. Wilson*, 503 U.S. 329 (1992))).

- The base offense level for the offense contained in Count Four is 6. *See* U.S.S.G. §§ 2X1.1, 2B1.1(a)(1).
- A 20-level enhancement is appropriate because the loss reasonably foreseeable to Khawar was more than \$7,000,000, but not more than \$20,000,000. *See* U.S.S.G. § 2B1.1(b)(1)(K).
- A 2-level enhancement is appropriate because (a) Khawar participated in relocating the fraudulent scheme to another jurisdiction to evade law enforcement or regulatory officials (*i.e.*, from the United Kingdom to the Netherlands), *and* (b) a substantial part of the fraudulent scheme was committed from outside the United States; *and* (c) the offense otherwise involved sophisticated means. *See* U.S.S.G. § 2B1.1(b)(10).
- A 2-level enhancement is appropriate because the offense involved (a) the possession or use of any (i) device-making equipment (*i.e.*, the credit card writer and associated software), or (ii) authentication feature (*i.e.*, the stolen PINs); *and* (b) the production of any (i) unauthorized access device or counterfeit access device, or (ii) authentication feature. *See* U.S.S.G. § 2B1.1(b)(11).

Assuming Khawar accepted responsibility for his crimes, therefore, the parties agreed that the total offense level on Count Four of the Indictment was 27. (PSR ¶¶ 42-54). Because Khawar has never lived in the United States, he has no American criminal history. (PSR ¶¶ 55-60). Accordingly, Khawar is in Criminal History Category I and the parties therefore stipulated – and the Probation Office agrees – that the appropriate Guidelines sentencing range for Khawar’s offense is 70-87 months’ imprisonment. (PSR ¶ 78).

**THE COURT SHOULD SENTENCE KHAWAR WITHIN THE GUIDELINES
RANGE OF 70 TO 87 MONTHS' IMPRISONMENT**

A. Applicable Law

A criminal sentence must be crafted to adequately reflect, among other things, the seriousness of the offense, the need for respect for the law, and the need to punish the offense and deter future criminal conduct. *See* 18 U.S.C. § 3553(a)(2). Based on the Guidelines calculations contained in the parties' plea agreement and in the PSR, the applicable Guidelines range is 70 to 87 months' imprisonment.

Although the Guidelines are of course no longer mandatory, the Supreme Court has made clear that a sentencing court should "consult" the Guidelines and "take them into account" when sentencing. *United States v. Booker*, 543 U.S. 220, 264 (2005). The Court has recently reaffirmed that the Sentencing Commission "continues to fill an important institutional role because it has the capacity courts lack to base its determinations on empirical data and national experience, guided by a professional staff with appropriate expertise. Accordingly, we have instructed that district courts must still give respectful consideration to the now-advisory Guidelines (and their accompanying policy statements)." *Pepper v. United States*, — U.S. —, 131 S.Ct. 1229, 1247 (2011) (internal quotation marks, citations, and alterations omitted). Indeed, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range," which "should be the starting point and the initial benchmark." *Gall v. United States*, 552 U.S. 38, 49 (2007); *see also United States v. Cavera*, 550 F.3d 180, 189 (2d Cir. 2008) (en banc) ("Even after *Gall* and *Kimbrough*, sentencing judges, certainly, are not free to ignore the Guidelines, or to treat them merely as a 'body of casual advice.'" (quoting *United States v. Crosby*, 397 F.3d 103, 113 (2d Cir. 2005))).

B. Discussion

Here, a Guidelines sentence is the right one. First and foremost, a Guidelines sentence is necessary to reflect the seriousness of Khawar's offense. Khawar played a significant – and arguably a leadership – role in an international credit card fraud conspiracy, recruiting and then traveling with his co-defendants from the United Kingdom to Holland on at least two occasions in order to install manipulated card readers at stores throughout Holland. Moreover, Khawar's prominent role came at a time when the Organization's original leadership was imprisoned, and he continued to participate in the fraud even after one of his friends (CC-5), whom he had personally recruited into the conspiracy, was arrested in his presence. Khawar therefore knowingly and wilfully continued to engage in blatantly criminal behavior, in the midst of an on-going international investigation, in order to perpetuate the fraud.

A Guidelines sentence is also necessary to deter future criminal conduct. The Organization of which Khawar was a part was extraordinarily sophisticated. They disseminated stolen account information to cashers throughout the world, but concentrated on the United States because its financial institutions are generally consumer-friendly. It was precisely because U.S. banks seek to please their customers — by having so many bank branches, by allowing large ATM transactions, and by permitting free movement throughout the country and often the world without presuming fraud on the part of the consumer — that the Organization targeted banks in New York City.

A Guidelines sentence is necessary in order to send the message that America will not allow its financial institutions to be victimized in this way. The news is replete with stories of criminals who use technology from abroad to prey on American victims in order to steal the personal and financial information of U.S. consumers. *See, e.g.,* Lily Hay Newman, "A

17-Year Old Was Behind the Target, Neiman Marcus Credit Card Hacks,” available at slate.com (Jan. 20, 2014) (describing Russian hacker who infiltrated at least eight large U.S. retail chains and accessed financial information about tens of millions of consumers); Elise Hu, “Analysts: Credit Card Hacking Goes Much Further than Target,” available at npr.com (Jan. 17, 2014) (describing prevalence of hacking directed at PEDs in U.S. retail locations).

A Guidelines sentence would also communicate that, regardless of who bears the ultimate financial loss, America will not tolerate crimes committed on its soil. That the Organization (although not Khawar) specifically relocated from Europe to the United States to take advantage of what it perceived to be easy victims and disinterested law enforcement only underscores the need for a sentence that will serve the goals of promoting respect for the laws and deterring future criminal conduct.

Khawar’s crime was a serious one, both in its own right and because his conduct occurred in the midst of a global financial crisis, when European financial institutions were particularly unstable. Moreover, once caught, Khawar lied to Dutch and American authorities in an attempt to minimize his own involvement, and in doing so, demonstrated further his lack of respect for the law. In fact, of the various co-conspirators with whom Khawar travelled to the Netherlands – including Fassel Azim, a “minor participant” whom Your Honor nonetheless previously (and appropriately) sentenced to 46 months’ imprisonment, (PSR ¶ 15) – he is plainly the most culpable.

Khawar is a defendant for whom a Guidelines sentence is necessary to afford adequate deterrence generally to criminal conduct and protect the public from his further crimes, as well as to reflect the seriousness of the offense and provide just punishment. *See* 18 U.S.C. § 3553(a)(1), (2)(A), (B) and (C).

CONCLUSION

For the foregoing reasons, the Government urges the Court to impose a sentence within the agreed Guidelines range of 70 to 87 months' imprisonment. In addition, the Court should impose orders of restitution and forfeiture, consistent with the recommendation contained in the PSR, copies of which will be provided to the Court at sentencing.

Dated: April 28, 2014
New York, New York

Respectfully submitted,

PREET BHARARA
United States Attorney

By: /s/ Matthew L. Schwartz
MATTHEW L. SCHWARTZ
NEGAR TEKEEI
Assistant United States Attorneys
One Saint Andrew's Plaza
New York, New York 10007
Telephone: (212) 637-1945/2482
Facsimile: (212) 637-2452
E-mail: matthew.schwartz@usdoj.gov
negar.tekeei@usdoj.gov